

**GENERAL SERVICES ADMINISTRATION**

**REQUEST FOR PROPOSAL  
47QTCB19P0006**

**For Services under 8(a) STARS II GWAC  
Constellation II, Functional Area 4**

**NAICS: 541519 - Other Computer Related Services**



**Issued by:  
Federal Acquisition Services  
Information Technology Category (ITC)  
1800 F Street NW  
Washington DC 20405-0001**

**RFP ISSUE DATE  
September 11, 2019**

**RFP CLOSE DATE  
September 19, 2019**

Solicitation#:47QTCB19P0006 QT3CDG Internal Security and System Security Assessment Support Services (ISSAS)

**SECTION A - SOLICITATION/CONTRACT FORM**

## **SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS**

### **NOTICE TO PROSPECTIVE OFFERORS**

The purpose of this Request for Proposal (RFP) is to secure the required Internal Security and System Security Assessment Support Services under the GSA 8(a) STARS II Governmentwide Acquisition Contract (GWAC) utilizing Constellation II, Functional Area 4 (NAICS 541519).

This resulting task order will be an 8(a) award under the authority in the STARS II GWAC in accordance with FAR 19.8. All services shall be performed in accordance with the terms and conditions of the Contractor's STARS II GWAC, this RFP and the resulting task order.

**All questions or requests for clarification shall be emailed to the Contract Specialist and Contracting officer by 4:00 p.m. Eastern Standard Time (EST) on September 16, 2019. Please cite the page number and specific solicitation section. Questions shall be sent to the following email addresses:**

**Jesse.Brassart@gsa.gov**  
**Contract Specialist**

**Leigh.Catella@gsa.gov**  
**Contracting Officer**

#### **B.1 GENERAL**

This is a non-personal services award to provide information technology (IT) security support services. The Government shall not exercise any supervision or control over the Contractor's employees performing the services herein.

This Task Order will be awarded and administered on a Labor Hour basis. The work shall be performed in accordance with all sections of this Task Order, the Performance Work Statement (PWS) and the Contractor's basic STARS II GWAC, under which the resulting Task Order will be placed.

**The Period of Performance shall not exceed 4 years and includes:**

#### **Internal Security Support Services:**

Base Period: Date of Award through 09/30/2020

Option Period 1: 10/01/2020 through 09/30/2021

Option Period 2: 10/01/2021 through 09/30/2022

Option Period 3: 10/01/2022 through 09/30/2023

The Option Periods will be awarded at the date of award, but not exercised. An Option is exercised when the Contracting Officer provides formal notification of the option exercise, via modification, to the successful offeror.

#### **B.2 SERVICES AND PRICES/COSTS**

The Offeror shall provide a labor hour proposal for services described in this RFP. The tables at Section B.2 below shall be used. All pricing submitted shall be inclusive of any applicable discounts offered from the Offeror's GSA STARS II GWAC rates. Specific instructions for completing the CLIN tables below are as follows:

- The Offeror shall enter their STARS II hourly rate in the column designated **"STARS II Labor Hour Rate."**
- The Offeror shall enter the proposed hourly rate in the column designated **"Proposed Labor Hour Rate" (this column should include any offered discounts).**

Solicitation#:47QTCB19P0006 QT3CDG Internal Security and System Security Assessment Support Services (ISSAS)

- The Offeror shall enter the total lump-sum extended amount for each CLIN in the column designated “Total CLIN Amount.”
- The Offeror shall enter the total evaluated price for the base and options in the last row designated “Total Evaluated Price.”
- The Offeror shall enter the totals from each period (base and options) in the table “Grand Totals,” and sum of the base and four option periods for the entire period of performance.

The Offeror is required to propose only labor categories awarded under their respective STARS II GWAC that will be used to enable the Offeror to fulfill this requirement. The proposed rates must be equal to or discounted from the rates awarded in the Contractor’s STARS II Price List.

**B.2.1 CLIN Tables:**

CLIN	Position Description(s) from 8(a) STARS II GWAC.	STARS II Labor Hour Rate	Quantity - Hours	Proposed Labor Hour Rate (Including offered discounts)	Total
0001 - Program Management (C.3.1)		\$		\$	\$
0002 - Information Assurance Support (C.3.2)				\$	\$
0003 - Systems Security Assessment Support (C.3.3)				\$	\$
	<b>TOTAL CEILING PRICE FOR BASE YEAR</b>				\$

CLINS	Position Description(s) and CLIN# from 8(a) STARS II GWAC.	STARS II Labor Hour Rate	Quantity - Hours	Proposed Labor Hour Rate (Including offered discounts)	Total
-------	------------------------------------------------------------	--------------------------	------------------	--------------------------------------------------------	-------

Solicitation#:47QTCB19P0006 QT3CDG Internal Security and System Security Assessment Support Services (ISSSAS)

1001- Program Management (C.3.1)				\$	\$
1002 - Information Assurance Support (C.3.2)				\$	\$
1003 - Systems Security Assessment Support (C.3.3)	N/A			\$	N/A
<b>TOTAL CEILING PRICE FOR OPTION YEAR 1</b>					<b>\$</b>

<b>CLIN</b>	<b>Position Description (s) and CLIN# STARS II GWAC.</b>	<b>STARS II Labor Hour Rate</b>	<b>Quantity - Hours</b>	<b>Proposed Labor Hour Rate (Including offered discounts)</b>	<b>Total</b>
2001 - Program Management (C.3.1)				\$	\$
2002 - Information Assurance Support (C.3.2)				\$	\$
2003 - Systems Security Assessment Support (C.3.3)	N/A			\$	N/A
<b>TOTAL CEILING PRICE FOR OPTION YEAR 2</b>					<b>\$</b>

<b>CLIN</b>	<b>Position Description and CLIN# from 8(a) STARS II GWAC.</b>	<b>STARS II Labor Hour Rate</b>	<b>Quantity - Hours</b>	<b>Proposed Labor Hour Rate (Including offered discounts)</b>	<b>Total</b>
-------------	--------------------------------------------------------------------------------	-----------------------------------------	-----------------------------	---------------------------------------------------------------------------	--------------

Solicitation#:47QTCB19P0006 QT3CDG Internal Security and System Security Assessment Support Services (ISSSAS)

3001- Program Management (C.3.1)				\$	\$
3002 - Information Assurance Support (C.3.2)				\$	\$
3003 - Systems Security Assessment Support (C.3.3)	N/A			\$	N/A
	TOTAL CEILING PRICE FOR OPTION YEAR 3				\$

TOTAL CEILING PRICE BASE & OPTIONS YEARS	\$
------------------------------------------	----

END OF SECTION B

## **SECTION C - PERFORMANCE WORK STATEMENT**

### **C.1 INTRODUCTION**

The General Services Administration (GSA) Federal Acquisition Service (FAS) Information Technology Category (ITC) Office of Telecommunications Services (OTS) develops and manages programs that meet the current and future telecommunications requirements of Federal agencies and departments. In addition, the Office of Telecommunications Services delivers administrative and technical support for services and solutions that are both efficient and cost-effective.

The Office of Telecommunications Services accomplishes this by:

Effectively leveraging competition to offer the best available telecommunications services and solutions at the best overall prices in the marketplace and Providing a customer focused, highly responsive, and fully integrated approach to helping Federal agencies.

Office of Telecommunications Services programs are available to Federal departments and agencies that meet the eligibility criteria contained in the GSA Directive ADM 4800.2G, Eligibility to Use GSA Sources of Supply and Services, dated September 17, 2009. Telecommunications services include data, voice, and video across a variety of transmission media such as radio, wire, cable, satellite, wireless. IT Security requirements must also be addressed.

The Office of Telecommunications Services currently offers the following technology contracts:

- [Networx \(Universal and Enterprise\)](#)  
Two broadly scoped acquisitions providing comprehensive service suites of telecommunication/IT services (will be replaced by the Enterprise Infrastructure Solutions [EIS] contracts).
- [Future COMSATCOM Commercial Services Acquisition \(FCSA\)](#)  
FCSA was created in partnership with the Department of Defense to create a multi-billion dollar common marketplace for the entire Federal Government to procure its commercial SATCOM services. It encompasses new Special Item Numbers on Federal Supply Schedule 70 and two new multiple-award ID/IQ contract vehicles, Custom SATCOM Solutions (CS2) and CS2-Small Business (CS2 and CS2SB will be replaced by CS3).
- [CONNECTIONS II \(CNX II\)](#)  
CNX III is a \$5 billion, 10-year multiple award contract that will be the Government's one-stop shop for obtaining telecommunications, network and communications solutions.
- [Federal Relay](#)  
Telecommunications access for Federal employees who are deaf, hard of hearing or speech disabled.
- [Telecommunications Expense Management Services \(TEMS\)](#)  
Convenient and single-source for ordering and managing wireless devices and service from regional or local carriers.
- [Local Telecommunications Services Contracts](#)  
Full range of first mile/last mile services and solutions.
- [Enterprise Infrastructure Solutions \(EIS\)](#)  
This acquisition is replacing GSA's current Networx Universal and Enterprise contracts as well as GSA Regional Local Service Agreements for government telecommunications and infrastructure solutions.

The Security Solutions Branch provides professional security services to GSA's internal and external clients with Information Security Officer (ISSO) support for the systems listed in Section C.3.2, personnel security, industrial security, as well as security consultant support to GSA (see Attachment "A" for the Security Solutions Branch Functional Responsibilities Matrix).

## **C.2.0 SCOPE**

The scope of work includes providing the GSA with comprehensive IT technical subject matter expert support to assist the Security Solutions Branch in ensuring contractual compliance with information assurance and IT security requirements and providing ongoing technical refreshment of the contracts listed in Section C.1 and any future acquisition initiatives assuring continued overall security compliance, and performing system security assessment services for the systems identified in Section C.3.3 and any future initiatives ensuring operational compliance.

- Perform all duties associated with an Information System Security Officer (ISSO). Reference Attachment “B”.
- Assist with development, reviews and maintenance of information system assessments and authorization (formerly known as Certification and Accreditation) documentation.
- Provide advice on emerging technologies and associated information assurance requirements.
- Review and provide recommended changes to newly developed/updated government guides, directives, policies and procedures (both Federal and Agency Level) relative to information assurance and security.
- Provide assistance with reviewing and updating contract deliverables associated with information assurance and security.
- Assist with the development of contract information assurance and IT security requirements relative to ITC programs.
- Support may also include attendance at security conferences/forums, technical research and analysis for presentations, white papers, position papers, and to brief the findings relative to information assurance and security.
- Provide independent third-party system security assessment services to include developing associated Security Assessment Reports.
- Perform system scans which include Web, Operating Systems and Database applications.
- Perform on-site inspections and interviews as required.
- Perform penetration tests to include developing associated reports.

## **C.2.1 OBJECTIVES**

The primary objective of the support to be provided under this task order is to ensure a solid, viable Information Assurance (IA) program for the systems that support our Government and Commercial clients. At a minimum our goals are to:

- Ensure accurate, timely, and quality personnel security documentation and processing for internal and external clients;
- Ensure accurate, timely, and professionally prepared industrial security documentation for internal and external clients;
- Ensure quality development, and reviews of all documents associated with systems security;
- Ensure accurate, thorough, and timely analysis of vulnerability scans and associated documentation; and
- Fully support the GSA CIO’s systems security efforts in accordance with all directives, security procedural guides, and standards.

## **C.3.0 TASK REQUIREMENTS**

### **C.3.1 Subtask 1 – Program Management**

The Contractor shall manage the tasks in this PWS in accordance with best practices established by the Program Management Institute (PMI), as described in the current PMI Project Management Body of Knowledge (PMBOK) Guide, and other applicable PMI publications and media. The Contractor shall perform management activities to include risk, quality, schedule, asset, and configuration management. The Contractor shall identify a Program Manager (PM), by name, who shall provide management, direction, administration, quality assurance, and leadership for the execution of this task order. The Contractor shall provide appropriately cleared, certified, trained,

and qualified personnel to support contract requirements, as well as all necessary personnel management services that are required to satisfy performance requirements.

#### **C.3.1.1 Subtask 1-1- Coordinate Task Order Kickoff Meeting**

The Contractor shall schedule and coordinate a Task Order Kick-Off Meeting at the location approved by the Government. The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved with the task order. The meeting will provide the opportunity to discuss technical, management, and IT security issues, and travel authorization and reporting procedures.

#### **C.3.1.2 Subtask 1-2 - Transition-In Plan**

The contractor shall provide a draft Transition-In Plan. The plan shall articulate as needed:

- The Contractor's transition approach, process and timelines.
- The Contractor's approach to mitigating or minimizing disruption.
- The Contractor's staffing status.
- Transition risk management and mitigation strategy
- Initial coordination with the prior Contractor.
- Gap analysis of required skills
- Training approach/knowledge transfer approach.

The Contractor shall execute its Government-approved Transition-in Plan. As part of this plan, the Contractor shall ensure there will be minimum service disruption to vital Government business and no service degradation during and after transition. All transition activities will be completed within 30 calendar days after the Project Kick-Off Meeting.

#### **C.3.1.3 Subtask 1-3 - Prepare Monthly Status Report (MSR)**

The Contractor Program Manager shall develop and provide a MSR using MS Office Suite of applications, by the 10<sup>th</sup> calendar day of each month via electronic mail to the Contracting Officer's Representative (COR). The report shall include the following:

- Activities during the reporting period, by task (Include: On-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- Personnel gains, losses and status (security clearance, etc.).
- Any government actions required.
- Schedule (Shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- Summary of any travel taken, conferences attended, etc. (Attach trip reports to this MSR for reporting period).
- Accumulated invoiced cost for each CLIN up to the previous month.
- Projected cost of each CLIN for the current month.

#### **C.3.1.4 Subtask 1-4 – Convene Technical Status Meetings**

The Contractor Program Manager shall convene a monthly Contract Activity and Status Meeting with the COR, and other key government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activity and status report, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The Contractor Program Manager shall provide

minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five (5) calendar days following each meeting.

#### **C.3.1.5 Subtask 1-5 - Prepare Program Management Plan (PMP) For Specific Taskings**

The Contractor shall submit a Program Management Plan (PMP) detailing how all aspects of the IT Services shall be obtained, how each of these activities shall be executed, and the Contractor's specific role in program execution. When required by the COR, the Contractor shall document all support requirements in a PMP for special projects/initiatives undertaken by the Security Solutions Branch that come up during the life-cycle of the task order. The PMP shall:

- Describe the proposed management approach.
- Include milestones, tasks, and subtasks required in this task order.
- Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations.
- Include the Contractor's Quality Control Plan (QCP) (if applicable).

The Contractor shall provide the Government with a draft PMP, on which the Government will make comments. The final PMP shall incorporate Government comments.

#### **C.3.1.6 Subtask 1- 6 - Prepare Trip Reports**

The Government will identify the need for a Trip Report (if required) when the request for travel is submitted (see Attachment "C"). A trip report will be due within 10 workdays following completion of each trip. The Contractor shall keep a summary of all long-distance travel, to include, at a minimum, the name of the employee, location of travel, duration of trip, and POC at travel location.

#### **C.3.2 Subtask 2 - Information Assurance Support**

The Contractor shall provide professional expertise in supporting requirements associated with Information Assurance (IA) and IT security requirements associated with the governments need to meet Federal Information Security Management Act (FISMA) mandates. This support will include but is not limited to reviews of IA and FISMA related security documentation associated with contract deliverables, GSA Security policies and procedures, assisting with Information Systems Security Officer (ISSO) requirements and attending related meetings, seminars and conferences. This support will require expert knowledge of Intelligence Community (IC), Department of Defense (DoD) as well as Federal Civilian Government policies and procedures. The Contractor shall also become thoroughly familiar with information assurance and security related policies and procedures for GSA as well as client agencies. The Security Solutions Branch currently requires IA and FISMA support associated with the following systems: Network Universal and Enterprise Contracts Operational Support Systems (OSS) for AT&T, CenturyLink, Level 3, and Verizon; MTIPS systems for AT&T, CenturyLink, and Verizon Business Services; Network Hosting Center (NHC); Conexus; Enterprise Infrastructure Services (EIS) Business Support Systems for AT&T, BT Federal, CenturyLink, Core Technologies, Granite, Harris Corporation, Manhattan Telecommunications (MetTel), MicroTech, and Verizon Business Network Services; EIS MTIPS for AT&T, BT Federal, CenturyLink, Granite, and Verizon Business Network Services, FedRelay, and Commercial Satellite Communications (CS3) contracts.

Support and deliverables associated with task area are:

- a. Provide assistance with creating and modifying Standard Operating Procedures for tasks associated with Security Assessments and Authorizations, continuous monitoring and annual reviews within 10 workdays of assignment by the COR.
- b. Provide assistance in developing and maintaining training plan for internal security staff within 10 workdays of assignment by the COR.

Solicitation#:47QTCB19P0006 QT3CDG Internal Security and System Security Assessment Support Services (ISSAS)

- c. Provide assistance in creating, modifying and maintaining, with 99.999 % accuracy, online dashboards related to the current security posture of and progress of deliverable submission for all systems owned by ITC within five (5) workdays as identified by the COR and maintaining on an on-going basis.
- d. Provide assistance with reviewing monthly/quarterly Plan of Actions & Milestones (POA&Ms) and associated system scans as well as submitting the review results to the GSA/FAS/CIO Security Office. The POA&Ms and scans shall also be posted to the GSA/OCIO/OCISO secure data storage sites (locations to be identified by the COR. Specific due dates for the quarterly POA&M reviews will be provided for each fiscal year as determined by the Chief Information Security Officer (CISO).
- e. Provide assistance with system security assessments/re-assessments and authorizations for Network OSSs, EIS BSSs, MTIPS, and other GSA systems as necessary to ensure that these systems retain their Authority-To-Operate (ATO). This includes reviewing System Security Plans (SSP) and associated appendices/attachments for accuracy and compliance. Documentation review reports due within five (5) to 10 workdays from receipt of SSP and associated appendices/attachments.
- f. Provide assistance with reviews and approvals of annual Contingency Test Plan Reports (CTPR) for supported systems – Report due within five (5) workdays from receipt of annual report.
- g. Provide assistance with reviews and approvals of annual Incident Response Test Reports (IRTR) for supported systems – Report due within five (5) workdays from receipt of annual report.
- h. Provide assistance with Annual FISMA Reviews and Data Calls for all ITC Office of Telecommunications Services systems to GSA/CIO – date varies dependent upon DHS/OMB requirements but normally occurs during June/July timeframe. Delivery of reviews due within 10 workdays after receipt of completed FISMA Reviews and Data Call documents.
- i. Provide reviews of all newly developed or updates to GSA IT Security Policies and Guides – report due within five (5) workdays after receipt of draft – final due dates determined by GSA/OCIO/OCISO.
- j. Provide assistance with preparation and delivery of final/approved versions of GSA Policies and Guide to appropriate Contractor Security Managers – review due within five (5) workdays after distribution by GSA/OCISO.
- k. Provide assistance with reviewing documentation associated with system modifications that affect system security posture – report due within five (5) workdays after receipt of modification documentation.
- l. Provides assistance with reviewing annual contract deliverables as well as other changes that may affect security posture that are submitted by program managers and system owners/security managers – reports due within five (5) of receipt of changed/updated documents.
- m. Provide assistance with the development of acquisition requirements and associated documentation related to FISMA, Information Assurance and Security within five (5) workdays of receipt of assignment.
- n. Attend NIST Federal Computer Security Program Managers (FCSPM) meetings – specific anticipated dates are provided by NIST each year – February, April, June (Annual Offsite), August, October and December (actual attendance dates posted about one month prior to meeting). A summary is due within five (5) workdays of completion of Meetings, Seminars, and Conferences
- o. Attend Security Conferences to enhance security knowledge and maintain security certifications and qualifications as necessary. A summary report is due within five (5) workdays of completion of Conferences.
- p. Provide Continuous Vulnerability Monitoring services for the systems associated with the Office of Telecommunication Services in accordance with GSA directives and security guides on an on-going basis.
- q. Reviews and provides input, at the government's request, on security-related documentation, or Incident Response reports as identified by the COR within five (5) workdays of assignment.

Note: All deliverables require 99.999 % accuracy.

The deliverables for this subtask are included in Section F.

### **C.3.3 Subtask 3 - Systems Security Assessment Support (As Required)**

Solicitation#:47QTCB19P0006 QT3CDG Internal Security and System Security Assessment Support Services (ISSSAS)

The contractor shall provide professional expertise in supporting requirements associated with the performance of system security assessments associated with the governments need to meet Federal Information Security Management Act (FISMA) mandates, all appropriate related government and agency policies, directives, security and hardening guides as well NIST Special Publications. This support will include but is not limited to reviews of System Security Plans and associated appendices/attachments; performance of database, web application and operating system scans when identified by the government; development of a Security Assessment Report (SAR), POA&M and associated authority to operate recommendation letters. This support will require expert knowledge of the Department of Defense (DoD), Federal Civilian Government, and Intelligence Community (IC) directives, policies, and procedures. The contractor shall also become thoroughly familiar with information assurance and security related policies and procedures for GSA as well as client agencies. The Security Solutions Branch is currently responsible for maintaining the Authorization to Operate for the following systems: Networx Universal and Enterprise Contracts Operational Support Systems (OSS) for AT&T, CenturyLink, Level 3, and Verizon; MTIPS systems for AT&T, CenturyLink, and Verizon Business Services; Network Hosting Center (NHC); Conexus; Enterprise Infrastructure Services (EIS) Business Support Systems for AT&T, BT Federal, CenturyLink, Core Technologies, Granite, Harris Corporation, Manhattan Telecommunications (MetTel), MicroTech, and Verizon Business Network Services; EIS MTIPS for AT&T, BT Federal, CenturyLink, Granite, and Verizon Business Network Services, and FedRelay. The listing of system security ATOs with their expiration dates are in Attachments "A" of this PWS. The number of system security assessments to be performed per month varies as noted in attachment "A", and it is possible that some of these assessments may occur simultaneously.

Support and deliverables associated with task area are:

- a. Set up, coordinate and perform security assessment initiation meeting where initial security assessment documentation will be provided to the third party assessment team. Due within five (5) workdays of receipt of system documentation.
- b. Develop a Security Assessment Plan (SAP) in accordance with GSA CIO IT Security Procedural Guide 06-30, Security Assessment and Authorization, Planning, and Risk Assessment. The SAP is due within ten (10) workdays of initiation meeting.
- c. Develop Rules of Engagement (RoE) for systems to be assessed. Due within five (5) workdays of the initiation meeting.
- d. Upon approval of SAP and RoE, perform security assessment to include scheduling of interviews, system scans as necessary and penetration testing.
- e. Conduct authenticated vulnerability scanning servers' operating systems when identified by GSA.
- f. Conduct authenticated vulnerability scanning of web servers when identified by GSA.
- g. Conduct authenticated vulnerability scanning of database servers when identified by GSA.
- h. Perform assess of security controls following the SAP and using the GSA Assessment Test Cases.
- i. Conduct configuration compliance scanning of all networking devices when identified by GSA. Scan results due within 15 workdays.
- j. Perform internal and external penetration testing to include Penetration Test Report (PTR). PTR is due within five (5) workdays of completion of tests.
- k. Develop a system security assessment Plan of Actions & Milestones (POA&Ms) to include all Critical, High and Moderate vulnerabilities identified during system scans. The POA&M is due within 20 workdays from completion of scans.
- l. Conduct code analysis to examine any developed software for common flaws and document the results in a Code Review Report when identified by GSA. This report will be due within five (5) days after completion of code analysis.
- m. Documentation review reports due within five (5) to 10 workdays of completion of site visits.

- n. Prepare a Security Assessment Report (SAR) documenting the issues, findings, and recommendations of the security control assessment. Document the assessment findings with recommendation(s) and risk determinations from the NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments. Draft SAR is due within 20 workdays of completion of site visits. Final version will be due within five (5) workdays of receipt of GSA comments.

Note: All deliverables require 99.999 % accuracy.  
The deliverables for this subtask are included in Section F.

#### **C.3.4 Subtask 4 - Surge Support (Optional Services)**

Due to the potential of significant increases in security workloads in any of the subtasks identified within this PWS, the contractor may be required to provide additional surge support to handle these additional requirements. All deliverables and performance measures will remain the same as currently identified in sections C.3.2 Subtask 2 - Information Assurance Support and C.3.3 Subtask 3 - Systems Security Assessment Support (As Required).

#### **C.3.5 ASSUMPTIONS**

This section defines the overall assumptions underlying this task which the Contractor should consider in developing their technical solutions to the subtasks in Section C.3:

- The Contractor shall use the available Government Furnished Information (GFI) and, where effective and appropriate, automated tools of the Office of Telecommunications Services (e.g., Networx Hosting Center) to analyze process and store contract sensitive and controlled unclassified information (CUI). Access to all relevant GFI will be provided after award.
- The Contractor shall consider Government requirements for IT security and privacy and their potential impact to service delivery during contract security requirements development processes.
- The Contractor may use any existing tool set made available by GSA or to which they have access in determining, documenting, and supporting their information assurance and IT security analyses.

**END OF SECTION C**

## **SECTION D – PACKAGING AND MARKING**

### **D.1 DELIVERABLES MEDIA**

The contractor shall provide electronic copies of each deliverable. Electronic copies shall be delivered via email attachment or other media by mutual agreement of the parties. The electronic copies shall be compatible with MS Office products or other applications as appropriate and mutually agreed to by the parties.

**END OF SECTION D**

## **SECTION E - INSPECTION AND ACCEPTANCE**

**NOTE:** The contractor's 8(a) STARS II GWAC is applicable to this task order and is hereby incorporated by reference. In addition, the following applies:

### **E.1 PLACE OF INSPECTION AND ACCEPTANCE**

Inspection and acceptance of all work performance, reports and other deliverables under this contract shall be in accordance with FAR 52.246-6, Inspection – Labor Hour and shall be performed by the GSA/FAS/ITC COR.

### **E.2 SCOPE OF INSPECTION**

1. All deliverables will be inspected for content, completeness, accuracy and conformance to contract requirements by the GSA/FAS/ITC COR.
2. The Government requires a period, not to exceed ten (10) workdays after receipt of final deliverable items for inspection and acceptance or rejection.

### **E.3 BASIS OF ACCEPTANCE**

1. The basis for acceptance shall be compliance with the requirements set forth in the contract, the contractor's proposal and other terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.
2. Reports, documents and narrative type deliverables will be accepted when all discrepancies, errors or other deficiencies identified in writing by the Government have been corrected.

### **E.4 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT**

The Government shall provide written notification of acceptance or rejection of all final deliverables within ten (10) working days (unless otherwise specified in Section F). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

### **E.5 NON-CONFORMING PRODUCTS OR SERVICES**

Non-conforming products or services will be rejected. Deficiencies will be corrected by the contractor, within three (3) workdays of the rejection notice. If the deficiencies cannot be corrected within three (3) work days, the contractor will immediately notify the GSA/FAS/ITC COR of the reason for the delay and provide a proposed corrective action plan within one (1) work day.

**END OF SECTION E**

## **SECTION F – DELIVERABLES AND/OR PERFORMANCE REQUIREMENTS**

### **F.1 DELIVERABLES**

All written deliverables require at least two iterations – a draft and a final. The final document must be approved and accepted by the Government prior to payment submittal. The vendor shall submit draft and final documents, using Microsoft Office 2003 or later, to the Government via email. The Government requires ten (10) business days for submission of written comments to the vendor and review on draft and final documents. The Contractor shall incorporate the Government's comments into draft and final deliverables before submission. Upon receipt of the Government comments, the Contractor shall have five business days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

Any issues that cannot be resolved by the vendor in a timely manner shall be identified and referred to the COR. The COR is designated by the Contracting Officer to perform technical liaison between the Contractor's management and the Contracting Officer in routine technical matters constituting general program direction within the scope of this Task Order. Under no circumstances is the COR authorized to effect any changes in the work required under this Task Order whatsoever, or enter into any agreement that has the effect of changing the terms and conditions of this Task Order or that causes the Contractor to incur any costs. In addition, the COR will not supervise, direct, or control Contractor employees. .

Notwithstanding this provision, to the extent the Contractor accepts any direction that constitutes a change to this Task Order without prior written authorization of the Contracting Officer, costs incurred in connection are at the sole risk of the Contractor, and are not allowable invoicing costs. On all matters that pertain to the Task Order terms, the Contractor must communicate directly with the Contracting Officer.

Whenever, in the opinion of the Contractor, the COR requests efforts beyond the terms of the Task Order, the Contractor shall so advise the Contracting Officer. If the COR persists and there still exists a disagreement as to proper contractual coverage, the Contracting Officer shall be notified immediately, preferably in writing. Proceeding with work without proper contractual coverage may result in non-payment or necessitate submittal of a claim.

Listed below are some of the possible deliverables that may be requested throughout the life of the resulting task order. Other deliverables that are considered within the scope of Section C.3 may also be requested.

<b>MILESTONE/DELIVERABLE</b>	<b>PWS Reference</b>	<b>PLANNED COMPLETION DATE</b>
Task Order Kickoff Meeting	C.3.1.1	At Task Order Award NLT 10 workdays after task order
Transition-In Plan	C.3.1.2	Within 30 calendar days after the Task Order Kick-Off Meeting
Monthly Status Report	C.3.1.3	Monthly (10th calendar day of the following month)
Monthly Technical Status Meeting	C.3.1.4	Monthly five (5) calendar days following each meeting)
Project Management Plan	C.3.1.5	As identified by the COR within five (5) workdays of assignment
Trip Report(s)	C.3.1.6	Within 10 workdays following completion of each trip

Solicitation#:47QTCB19P0006 QT3CDG Internal Security and System Security Assessment Support Services (ISSSAS)

Creating and modifying Standard Operating Procedures	C.3.2.a.	Within 10 workdays of assignment by the COR with 99.999% accuracy
Development and maintenance of training plans	C.3.2.b.	Within 10 workdays of assignment by the COR with 99.999% accuracy
Creation, modification, and maintenance of online dashboards	C.3.2.c.	Within five (5) workdays as identified by the COR and maintaining on an on-going basis
Monthly/Quarterly Review Status Reports	C.3.2.d.	Within 10 workdays of receipt of documentation with 99.999 % accuracy
Report of Security Assessment / Reassessment Documentation Reviews	C.3.2.e.	Within 10 workdays of receipt of documentation with 99.999 % accuracy
Report of Annual Contingency Test Plan Report Reviews	C.3.2.f.	Within five (5) workdays of receipt of Annual Report with 99.999 % accuracy
Report of Annual Incident Response Plan Test Report Reviews	C.3.2.g.	Within five (5) workdays of receipt of IRPT with 99.999 % accuracy
Report of Annual FISMA Reviews and Data Calls	C.3.2.h.	Within 10 workdays of receipt of FISMA Review and Data Calls with 99.999 % accuracy
Report of GSA Policy and Procedure Reviews and Distribution	C.3.2.i. & j.	Within five (5) workdays after distribution by GSA/OCISO with 99.999 % accuracy
Report of System Modification Reviews	C.3.2.k.	Within five (5) workdays after receipt of modification documentation with 99.999 % accuracy
Reports for Reviews of Contract Security Related Deliverables	C.3.2.l.	Within five (5) of receipt of changed/updated documents
Report of FISMA, and Information Assurance and Security related Acquisition Requirements and associated documentation developed	C.3.2.m.	Within five (5) workdays of receipt of assignment with 99.999 % accuracy
Summary of Meetings, Seminars and Conferences Attended	C.3.2.n. & o.	Within five (5) workdays of completion of Meetings, Seminars, and Conferences with 99.999 % accuracy
Continuous Monitoring Status Reports	C.3.2.p.	On an on-going basis with 99.999 % accuracy
Review reports of security-related Documentation, and Incident Response reports	C.3.2.q.	As identified by the COR within five (5) workdays of assignment with 99.999 % accuracy
Scheduling of Security Initiation Meetings	C.3.3.a	Within five (5) workdays of receipt of accepted system documentation with 99.999% accuracy
Security Assessment Plan (SAP)	C.3.3.b	Within 10 workdays of initiation meeting with 99.999% accuracy

Solicitation#:47QTCB19P0006 QT3CDG Internal Security and System Security Assessment Support Services (ISSSAS)

Rules of Engagement (RoE)	C.3.3.c	Within five (5) workdays of initiation meeting with 99.999% accuracy
Reports from Authenticated Vulnerability Scans of Server Operating Systems	C.3.3.e	Within 10 workdays after completion of scans with 99.999% accuracy
Reports from Authenticated Vulnerability Scans of Web Servers	C.3.3.f	Within 10 workdays after completion of scans with 99.999% accuracy
Reports from Authenticated Vulnerability Scans of Database Servers	C.3.3.g	Within 10 workdays after completion of scans with 99.999% accuracy
Report from Configuration Compliance Scans	C.3.3.i	Within five (5) workdays after completion of scans with 99.999% accuracy
Internal and External Penetration Test Reports (PTR).	C.3.3.j	Within 15 workdays of completion of tests with 99.999% accuracy
Security Assessment POA&M	C.3.3.k	Within 20 workdays of completion of scans with 99.999% accuracy
Code Analysis Report	C.3.3.l	Within five (5) workdays of completion of code analysis
Documentation Review Reports	C.3.3.m	Within 10 workdays after completion of visits with 99.999% accuracy
Security Assessment Report	C.3.3.n	Draft within 20 workdays of completion of site visits. Final version due within five (5) workdays of receipt of GSA comment with 99.999% accuracys.

## F.2 PLACE OF PERFORMANCE

The primary place of performance shall be in the Government's location at GSA Headquarters, 1800 F Street, N.W. Washington, D.C. 20405. At a minimum, hoteling space will be provided for two days per week.

The Contractor's Employee(s), when conducting business on a Government-furnished (i.e., Government-issued) or approved computer/laptop, may be allowed to work at an alternate work location (including the Contractor's facility) that is not a "Federally-controlled facility" as coordinated by the Contracting Officer's Representative (COR).

In order to meet Zero Environmental Footprint goals, ensure a sustainable workplace, and facilitate a mobile workforce, GSA has reduced the amount of real estate space used to house its workforce in the Washington, DC Metro Area. Part of the solution to this problem was to reduce the amount of desk space used by contract workers supporting GSA. All new service contract solicitations will require the Contractor to designate a location other than a GSA facility as an alternate primary place of performance (telework site).

## F.3 PERFORMANCE MEASURES

Through various means the Government will be conducting quality assurance to ensure the Contractor is providing the requisite level of service to Government staff. The aforementioned quality ensure may be through customer surveys, inquiries made to other Government offices, or through customer comments.

Measures given below must be adhered to at all times during the performance of the Task Order. However, the FINAL performance measures will be determined by the government and the awarded Contractor.

The success of this RFP shall be dependent upon the Government's Quality Assurance Service Plan (QASP) provided and shall depend on the following performance measures:

- **Quality of the deliverables** - This includes their accuracy as well as their presentation, completeness and general quality of production. The products should contain approaches and solutions and clearly show how the Contractor has made an effort to provide as comprehensive an approach as possible. The contractor shall advise the Office of Telecommunications Services (OTS) of quality issues, apply and document quality assurance procedures and methodologies to ensure that client quality requirements and performance standards are clearly met and effectively enforced.
- **Timeliness of the deliverables** - Once a firm schedule is established, adherence to the timeline is important to meet the overall objectives of the task.

#### F.4 PERFORMANCE MANAGEMENT METRICS

On a monthly basis, the Contractor shall meet the performance objectives listed in the table below. Any deliverable(s) or non-performing service(s) that do not meet the Performance Measure and associated Inspection and Acceptance Criteria shall be repaired/replaced/re-performed by the Contractor in accordance with FAR Clause 52.212-4 Alt 1.

##### Explanation of Columns

Performance Requirement:	A specific task to be completed, or deliverable to be furnished.
Performance Indicator:	An indicator or particular aspect of the Contractor's task performance that will be looked at to determine whether the requirement has been successfully performed.
Performance Standard:	Standard represents the performance baseline against which the Contractor will be measured.
Performance Surveillance:	The method used to measure Contractor's performance Methodology (source, or data collection method)

Performance Requirement	Performance Indicator	Performance Standard	Performance Surveillance Method
Monthly Status Report (MSR) (Task C.3.1.2)	Deliver complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Project Management Plan (Task C.3.1.4)	Deliver complete and on time	Clarity, accuracy and contains all the data required.	100 % Inspection of Each PMP

Solicitation#:47QTCB19P0006 QT3CDG Internal Security and System Security Assessment Support Services (ISSSAS)

		Initial deliverable submission shall be 90% error free.	
Miscellaneous Administrative Reports (Tasks C.3.1.3 and C.3.1.5)	Deliver complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Monthly/Quarterly Plan of Action and Milestone (POA&M) Reviews (Task C.3.2.a)	Deliver complete and on time	Clarity, accuracy, contains all the data required. In compliance with applicable Government and GSA directives/policies and procedural guides, OMB Memorandums and NIST Special Publications.  Initial deliverable submission shall be 90% error free.	100 % Inspection of All Documents
Review of Assessment & Authorization Documentation (Tasks .C.3.2.b, C.3.2.c, and C.3.2.d)	Deliver complete and on time	Clarity, accuracy, contains all the data required. In compliance with applicable Government and GSA policies/guideline and NIST Special Publications. Initial deliverable submission shall be 90% error free.	100 % Inspection of All Documents
Review Report of Annual FISMA Reviews and Data Call (Task C.3.2.e)	Deliver complete and on time	Clarity, accuracy, contains all the data required. In compliance with applicable Government and GSA policies/guidelines, OMB memorandum and NIST Special Publications. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Report of reviews of newly developed and updated GSA Security Policies and Guides (Task C.3.2.f)	Deliver complete and on time	Clarity, accuracy, contains all the data required. In compliance with applicable GSA policies. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Report of Reviews of system modifications (C.3.2.h)	Deliver complete and on time	Clarity, accuracy, contains all the data required. In compliance with applicable Government and GSA policies/guidelines, OMB memorandum and NIST Special Publications. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports and affected Documents
Contract Annual Deliverables Review Report (Task C.3.2.i)	Deliver complete and on time	Clarity, accuracy, contains all the data required. In compliance with applicable Government and GSA policies/guidelines, OMB	100 % Inspection of Reports and affected Documents

Solicitation#:47QTCB19P0006 QT3CDG Internal Security and System Security Assessment Support Services (ISSSAS)

		memorandum and NIST Special Publications. Initial deliverable submission shall be 90% error free.	
Report of FISMA, and Information Assurance and Security related Acquisition Requirements and associated documentation developed (Task C.3.2.j)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Summary Report of Meetings, Seminars and Conferences Attended (Task C.3.2.k. and C.3.2.l.)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Continuous Monitoring Status Reports (Task C.3.2.m.)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Review reports of Security related documentation, or Security Incident Response reports (Task C.3.2.n.)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Scheduling of Security Initiation Meetings (Task C.3.3.a)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Security Assessment Plan (SAP) (Task C.3.3.b)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Rules of Engagement (RoE) (Task C.3.3.c)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Authenticated Vulnerability Scans of Servers' Operating Systems (Task C.3.3.e)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Authenticated Vulnerability Scans of Web Servers	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall	100 % Inspection of Reports

(Task C.3.3.f)		be 90% error free.	
Authenticated Vulnerability Scans of Database Servers (Task C.3.3.g)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Configuration Compliance Scans (Task C.3.3.i)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Internal and External Penetration Test Reports (PTR) (Task C.3.3.j)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Security Assessment POA&M (Task C.3.3.k)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Code Analysis Report (Task C.3.3.l)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Documentation Review Reports (Task C.3.3.m)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports
Security Assessment Report (Task C.3.3.n)	Deliver Complete and on time	Clarity, accuracy and contains all the data required. Initial deliverable submission shall be 90% error free.	100 % Inspection of Reports

## F.5 QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

### F.5.1 Objective

The purpose of this plan is to provide a quality assurance surveillance plan for use by the COR assessing the quality of both the support and deliverables being provided to the OTS. This plan provides a basis for the COR to evaluate the quality of the Contractor's performance. The oversight provided for in the task order and in this plan will help to ensure that service levels reach and maintain the required levels throughout the task order term. Further, this plan provides the COR with a proactive way to avoid unacceptable or deficient performance, and provides verifiable input for the required performance evaluations.

### F.5.2 Work Requiring Surveillance and Method of Surveillance

All of the deliverables listed above and defined for each specific project will be surveilled by the COR via visual inspection. The Government shall also take the following actions to ensure quality Contractor performance under the resulting task order:

- A. **Performance Monitoring.** The Contractor is required to provide sufficient qualified personnel to perform the requirements of the task order. Customer feedback will be sought. Further, the COR will review

measures taken by the Contractor to keep all customers informed of situations that may affect performance and schedules.

The COR will analyze the performance measure data collected by the government for each performance period. The COR will perform the quality assurance functions to ensure the Contractor is providing an acceptable level of service to the government. The quality assurance functions will also include inspecting deliverables for both quality and timeliness.

- B. **Review of Travel Costs.** The COR will review all travel vouchers submitted with invoices. In addition, the COR may periodically request a review of travel vouchers by an independent party to ensure that the Contractor follows the Federal Travel Regulation (FTR). Such reviews will occur at least annually.
- C. **Consultation With The Contractor.** The COR will meet with the Contractor's Project Manager and the Contractor's Task Leads each month to: Discuss any problems; identify circumstances beyond the control of the Contractor; identify possible remedies; and note positive accomplishments. The COR will document the meeting.

**END OF SECTION F**

## **SECTION G - CONTRACT ADMINISTRATION DATA**

### **G.1 INVOICES/PAYMENTS**

The contractor shall submit invoices using the GSA Vendor and Customer Self Service website at <https://vcss.ocfo.gsa.gov/>. In order to be considered proper for payment, invoices shall be submitted in accordance with the following instructions and 52.232-1 Payments:

- Invoices shall be submitted monthly, unless otherwise specified, to the designated billing office specified in the resulting contract.
- Invoices must include the Accounting Control Transaction (ACT) number provided on the resulting contract.

Invoices are authorized for payment upon the Government's receipt and acceptance of deliverables specified in the contract and the receipt of a valid invoice. Invoices must include the following:

- Name and address of the Contractor
- Invoice date and number
- Name, address, phone number and email address of official to whom payment is to be sent
- Name, title, phone number and email address of person to be notified in the event of defective invoice
- Contract Number: (From GSA Form 300, Block 2)
- TP Number (ACT Number): (From GSA Form 300, Block 4)
- Invoice Number
- Period of performance covered by the invoice
- CLIN titles
- CLIN numbers
- Cumulative Number of Hours (by CLIN)
- Fixed Hourly Rate/Unit Price (by CLIN)
- Invoice Amount (by CLIN)
- Project Code (by Task Area)
- Current Charges (by Project Code Number)
- Charges to Date (by CLIN)
- Total Invoice Amount
- Description of the services provided including separate cost detail for each employee/Contractor personnel, quantity, unit of measure, unit price and extended price of the item(s) delivered; period of service and/or dates that services were provided, etc., in addition to the associated CLIN-based data required by the Terms of Reference (TOR), which may be the same.
- Taxpayer Identification Number (TIN). The Contractor will include its TIN on the invoice only if required elsewhere in this contract.

A duplicate electronic invoice with supporting documentation is sent to the COR and the Contracting Officer. The COR will confirm deliveries or performance made against the invoice line items to ensure that the correct amounts have been billed and will document any price deductions. The COR will then certify (using the COR stamp) and provide signature indicating that the invoice is valid for payment. Invoices are authorized for payment upon the Government's receipt and acceptance of deliverables specified in the contract and the receipt of a valid invoice.

Invoices will be rendered no later than the 25th calendar day of the month following performance and must be accompanied by all status reports submitted during that period. The COR must receive a copy of the invoice and all supporting documentation before or at the same time as the GSA Finance Office.

### **G.2 GSA POINTS OF CONTACT**

Solicitation#:47QTCB19P0006 QT3CDG Internal Security and System Security Assessment Support Services (ISSSAS)

The GSA COR provides technical review of deliverables, invoice servicing and facilitating payment. The GSA Contracting Officer's Representative (COR) is:

William (Bill) Olson  
Phone: 703-306-6393  
E-mail: William.Olson@gsa.gov

The GSA CO has overall responsibility for administering the Task Order. All Task Order administration shall be performed by the GSA CO. The GSA Contracting Officer is:

Contracting Officer: Leigh Catella  
Phone: 202-285-9127  
Email: Leigh.Catella@gsa.gov

Contract Specialist: Jesse Brassart  
Phone: 202-374-9509  
Email: Jesse.Brassart@gsa.gov

**END OF SECTION G**

## **SECTION H - SPECIAL CONTRACT REQUIREMENTS**

### **H.1.0 KEY PERSONNEL**

The following positions are designated key personnel for this task order:

- Program Manager
- IT Systems Security Subject Matter Specialist
- Senior Security Analyst
- Systems Analyst
- Test Analyst

The offeror shall propose the appropriate labor category for these positions or their equivalent from its 8(a) STARS II Contract.

### **H.1.1 Key Personnel Substitution**

The Contractor shall not remove or replace any personnel designated as key personnel for this task order, without the written concurrence of the CO. Prior to utilizing other than personnel as specified in response to a RFP, the Contractor shall notify the CO and the GSA/FAS/ITC COR. This notification shall be no later than ten (10) calendar days in advance of any proposed substitution, and shall include justification, including resume(s) and labor category of each proposed substitution(s) in sufficient detail to permit evaluation of the impact on task order performance.

Substitute personnel qualifications shall be equal to, or greater than, the qualifications of the personnel being substituted. If the CO and the GSA/FAS/ITC COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the task order, the Contractor may be subject to default action as prescribed by FAR 52.212-4 Alt

### **H.1.2 Labor Categories**

Critical to the performance of this contract are the positions identified on this Task order as key and the relevant experience of the people in those positions. The proposed key position(s) (see H.1.2) as well as proposed staff shall show relevant experience in the different skill sets necessary and the different functions to be performed.

- The Contractor shall identify the key Contractor personnel. The key personnel shall be maintained through completion of the contract and be responsible for all activities under this contract. This should describe the proposed action (including resignation, if applicable), any corresponding transition plan, and assessment of the anticipated impact to the program efforts; and
- The Contractor shall provide the resume(s) for the proposed change to the appropriate PM and COR for evaluation and possible interview before acceptance by the Government.

### **H.1.3 Replacement of Key Personnel**

All personnel on this contract, upon ordering of services and will require approval of the position to the project by the Contracting Officer (CO).

Replacement of Key personnel can be disruptive and interfere with the government's ability to accomplish the efforts in a timely manner. The potential impacts of a Key personnel replacement can sideline the mission and impact the goals of the affected Program office for a substantial amount of time. The Contractor shall not remove or replace any personnel designated as key personnel for this Task Order, without the written concurrence of the CO. Prior to utilizing other than personnel specified in proposals in response to a RFP, the Contractor shall notify

the appropriate COR. This notification shall be no later than fifteen (15) calendar days in advance of any proposed substitution, and shall include:

1. Justification for the proposed substitution should:
  - a. Address what are the circumstances surrounding the individual's departure;
  - b. Give a reason why it is believed to be in the government's best interest to accept such a change.
  - c. Explain how the government can expect to maintain continuity in the efforts that are ongoing considering the retraining and re-familiarization with our organization and assigned tasks that inevitably has to happen with the introduction of any new individual.
2. The labor category of each proposed substitution.
3. A detailed resume for each proposed substitution to permit evaluation of the impact on Task Order performance.

Keep in mind that if the CO and GSA/FAS/ITS COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the task order, the Contractor may be subject to default action as prescribed by FAR 52.212-4 Alt I.

Key personnel are designated Key because they are deemed crucial to the mission and overall success of the program. Key personnel substitutions are scrutinized with higher rigor than perhaps, non-key personnel on a contract. Requests for replacement shall also include a detailed resume containing a description of position duties and qualifications, information about the qualifications of the individual(s) proposed, and any additional information requested by the Contracting Officer in sufficient detail to permit the Contracting Officer to evaluate the impact on the work the Contractor is obligated to perform hereunder.

*Key Personnel* substitutions should be accompanied by convincing assurances that the Contractor has proposed a replacement individual **whose qualifications meet or exceed those of the previous individual** in that labor category and position. They are *not compared with the original contract requirements*.

#### **H.1.4 Key Personnel Assignments**

All key personnel are subject to the following:

- The Contractor shall provide staff to ensure all work is performed on schedule and by following best commercial practices.
- The Contractor may move around the personnel to different roles/responsibilities, if necessary, upon COR's approval.
- The list of key personnel set forth may be amended from time to time during the course of the Task Order to either add or delete personnel, as appropriate.

#### **H.1.5 Personnel Requirements**

The Contractor shall provide staff to ensure all work is performed on schedule in accordance with the deliverables list. All staff interfacing with the Government shall be fluent in the English language, verbal and written.

#### **H.1.6 Contracting Officer's Authority**

The Contracting Officer is the only person authorized to approve changes in any of the requirements of the Task Order.

## **H.2 GOVERNMENT FURNISHED ITEMS**

### **H.2.1 Government Furnished Space**

The Government will provide, as necessary, on-site office facilities to include hoteling space and basic office configuration, which includes: laptop and docking station, printer, desk, chair, basic office supplies, internet connection and local telephone service for Contractor personnel.

### **H.2.2 Government Furnished Equipment**

The Government will provide as necessary, the basic space and equipment listed above for on-site work. The laptop will be used for off-site work, as required.

## **H.3 PERSONNEL ACCESS TO GOVERNMENT INFORMATION AND FACILITIES AND BACKGROUND INVESTIGATIONS**

For any Contractor personnel performing work under this PWS who shall require access to GSA IT applications, systems, or data, the Contractor(s) shall comply with the Homeland Security Presidential Directive-12 (HSPD-12) security clearance process. This means first obtaining an Enter on Duty Determination (EoDD), which typically takes three (3) to four (4) weeks. At that point, the COR or Program Manager can grant limited access on a case-by-case basis. Only when a full adjudication is received shall full access be granted. This process usually takes four (4) to eight (8) months, although it could take as many as 12 months.

Contractor proposed personnel shall have at a minimum of a Tier 2 S (formerly Minimum Background Investigation - MBI) background investigation Contractor(s) shall not be granted unescorted access to a GSA facility or to any GSA IT system prior to receiving an EoDD.

The Contracting Officer or COR retains the right to request removal of Contractor personnel, regardless of prior clearance or adjudication status, whose actions, while assigned to Task Orders, clearly conflict with the interest of the Government.

## **H.4 NOTICE OF ORDER SIZE RE-REPRESENTATION (OSR) AT THE TASK ORDER LEVEL**

Offers are solicited only from 8(a) STARS GWAC prime Contractors that have not Re-Represented as other than small in accordance with FAR 52.219-28 Post-Award Small Business Program Rerepresentation. Those 8(a) STARS GWAC prime Contractors having experienced an event that triggers the notification requirements contained in FAR 52.219-28(b)(1) or (b)(2), and are other than small as a result of said triggering event, are considered to be other than a small business concern for the purposes of this procurement regardless of whether the Contractor has fulfilled the re-representation notification pursuant to FAR 52.219-28.

Offers received from 8(a) STARS GWAC Contractors that have represented their size status as other than small under the 8(a) STARS GWAC, or have had a triggering event and are not currently considered small business concerns under the 8(a) STARS GWAC are not desired and shall be rejected as non-conforming with this OSR.

## **H.5 MINIMUM QUALIFICATIONS**

Vendors should propose their most qualified and experienced personnel based on the best fit for the work requirements, keeping in mind that the Government believes the best fit to be personnel with the following qualifications and pertinent work experience. (Roles and Responsibilities may be used, in keeping with the 8(a) Stars II contract model).

### **H.5.1 Program Manager:**

- Bachelor's Degree in computer science, IT Security, or a related field, or a combination of education and experience equivalent to a Bachelor's degree.
- Seven (7) or more years of relevant experience in organizational planning or related field and actual performance as a Program Manager

- Desired Certifications include, Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Project Management Professional (PMP – PMI), or equivalent.

#### **H.5.2 IT Systems Security Subject Matter Specialist:**

- Bachelor's Degree in computer science or a related field
- Five (5) or more years of relevant experience in the development, test, or operations of software, platform or in emerging technology and innovation
- Desired Certifications include, Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Project Management Professional (PMP – PMI), or equivalent.

#### **H.5.3 Senior Security Analyst:**

- Bachelor's Degree in computer science or a related field or a combination of education and experience equivalent to a Bachelor's degree.
- Seven (7) or more years of relevant experience in managing system security assessments or related system security functions.
- Desired Certifications include, Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Project Management Professional (PMP – PMI), or equivalent.

#### **H.5.4 Security Systems Analyst:**

- Bachelor's Degree in computer science or a related field or a combination of education and experience equivalent to a Bachelor's degree.
- Five (5) or more years of relevant experience in performing system security assessments
- Desired Certifications include, Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Project Management Professional (PMP – PMI), or equivalent.

#### **H.5.5 Test Analyst:**

- Bachelor's Degree in computer science or a related field or a combination of education and experience equivalent to a Bachelor's degree.
- Five (5) or more years of relevant experience in performing system security assessments
- Desired Certifications include, Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Project Management Professional (PMP – PMI), or equivalent.

### **H.6 SENSITIVE INFORMATION STORAGE**

Controlled Unclassified Information (CUI), data, and/or equipment will only be disclosed to authorized personnel on a Need-To-Know basis. The Contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment shall be returned to the Government.

The Government will determine the fate of such information, data, and/or equipment. If the Government determines that such information, data, and/or equipment is to be destroyed, the destruction shall be accomplished by burning; shredding or any other method that precludes the reconstruction of the material but only after direction by the Government. All sensitive information contained on Contractor computers shall be either degaussed or shall be handled in accordance with NIST 800-88, Guidelines for Media Sanitization.

The Contractor shall adhere to all information staff and facility security requirements in accordance with GSA Order CIO 2100.3B Mandatory, IT Security Training Requirement for Agency Contractor Employees with Significant Security Responsibilities and GSA IT General Rules of Behavior GSA Order CIO 2104.1A. The Contractor shall also comply with each application's security requirements.

All works in the tasking identified in this SOW are unclassified or carry Privacy Act classification. The data that the Contractor shall have access to may have relatively high sensitivity. As a result, the Contractor shall be required to sign a nondisclosure agreement relating to sensitive data.

Employee Clearances- Background investigation requirements for access to GSA information systems (including Contractor operations containing GSA information) shall be in accordance with the GSA Order P 2181.1 Homeland Security Presidential Directive 12 Personal Identity Verification & Credentialing Handbook. The Contractor is also required to notify the Government whenever a cleared person is terminated.

The Contracting Officer or COR retains the right to request removal of Contractor personnel, regardless of prior clearance or adjudication status, whose actions, while assigned to contracts, clearly conflict with the interest of the Government. All costs associated with obtaining HSPD-12 credentials are absorbed by the Contractor.

## **H.7 PROTECTION OF INFORMATION**

The Contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this Task Order. The Contractor shall also protect all Government data, equipment, etc. by treating the information as sensitive. All information about the systems gathered or created under this Task Order should be considered as CUI. It is anticipated that this information will be gathered, created, and stored within the primary work location. If Contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

The government will retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

The data must be available to the Government upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The Contractor shall provide requested data at no additional cost to the government.

No data shall be released by the Contractor without the consent of the Government in writing. All requests for release must be submitted in writing to the COR/CO.

## **H.8 PERSONNEL SECURITY CLEARANCES**

It is anticipated that certain work may require a security clearance of up to a Top Secret/SCI. All guidance on security shall be in accordance with the draft Department of Defense Contract Security Classification Specification (DD Form 254, see Attachment "F").

## **H.9 CONFIDENTIALITY AND NONDISCLOSURE**

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the Contractor in the performance of this Task Order, are the property of the U.S. Government and must be submitted to the COR at the conclusion of the Task Order.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced, or retained by the Contractor. All appropriate project documentation will be given to the agency during and at the end of this Task Order. The Contractor shall not release any information without the written consent of the Contracting Officer.

The contractor's employees assigned to under this contract shall be required to sign contract specific Nondisclosure Agreements (NDAs) and Individual Conflict of Interest (COI) forms in line with this Organization Conflict of Interest clause.

#### **H.10 GENERAL COMPLIANCE REQUIREMENTS**

GSA information systems are the property of the Government. The Contractor shall be responsible for adhering to all aspects of the Privacy Act and is prohibited from removing from the worksite any programs, documentation, or data without the knowledge AND written approval of the COR.

#### **H.11 GSA CHIEF INFORMATION OFFICER (CIO) POLICIES**

The following GSA CIO policies shall be followed during Task Order performance:

- CIO P 1878.2A Conducting Privacy Impact Assessments (PIAs) in GSA
- CIO P 2100.1 GSA Information Technology (IT) Security Policy
- CIO 2106.1 GSA Social Media Policy
- CIO 2160.4A Provisioning of Information Technology (IT) Devices
- CIO 2162.1 Digital Signatures
- CIO P 2165.2 GSA Telecommunications Policy
- CIO P 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
- (8) CIO 9297.1 GSA Data Release Policy
- (9) CIO 9297.28 GSA Information Breach Notification Policy

All GSA policies listed in this paragraph must be followed, when inside a GSA building or inside a GSA firewall:

- CIO P 2100.28 GSA Wireless Local Area Network (LAN) Security
- CIO 2100.38 Mandatory Information Technology (IT) Security Training
- Requirement for Agency and Contractor Employees with Significant Security Responsibilities
- CIO 2104.1A GSA Information Technology IT General Rules of Behavior
- CIO 2182.2 Mandatory Use of Personal Identity Verification (PIV) Credentials
- ADM P 9732.1 D Suitability and Personnel Security

### **END OF SECTION H**

## **SECTION I - CLAUSES AND PROVISIONS**

#### **I.1 TYPE AND TERM OF CONTRACT**

The General Services Administration anticipates awarding a Labor Hour Task Order for providing the services requested in this RFP. The term of the Task Order includes a base period of one (1) year with three (3) one (1) year options.

#### **I.2 ORGANIZATIONAL CONFLICT OF INTEREST (see Attachment "D")**

##### **I.2.1 PURPOSE**

The purpose of this clause is to protect the integrity of the procurement by ensuring that a Contractor does not obtain any unfair competitive advantage over other parties by virtue of its performance under this Task Order and is not able to manipulate a competition for a Government contract or Task Order to its favor.

### **I.2.2 SCOPE**

The restrictions described herein apply to performance or participation by the Contractor and any of its affiliates or their successors in interest (hereinafter collectively referred to as "Contractor") in the activities covered by this clause as a prime Contractor, subcontractor, co-sponsor, participant in a joint venture, consultant, or in any similar capacity. For the purpose of this clause, affiliation occurs when a business concern is controlled by or has the power to control another or when a third party has the power to control both. Further, the Contractor may be required to describe to GSA how it will comply with the following limitations.

### **I.2.3 ACCESS TO AND USE OF INFORMATION**

If the Contractor, in the performance of this Task Order, obtains access to information, such as GSA or Contractor plans, policies, reports, studies, financial plans, internal data protected by the Privacy Act of 1974 (5 U.S.C. 552a), or proprietary data which has not been released or otherwise made available to the public, the Contractor agrees that it may not (without prior written approval of the contracting officer):

- i Use such information for any private purpose including but not limited to consulting services, advisory services, or responses to fair opportunity Task Order processes unless the information has been released or otherwise made available to the public;
- ii Compete for work for any federal agency based on such information for a period of one (1) year after GSA closes out the Task Order with the Contractor;
- iii Submit an unsolicited proposal to any federal agency which is based on such information until one (1) year after such information is released or otherwise made available to the public; and
- iv Release such information unless such information has been previously released or otherwise made available to the public by GSA.

In addition, the Contractor agrees that to the extent it receives or is given access to proprietary data, data protected by the Privacy Act of 1974 (5 U.S.C. 552a), or other confidential or to privileged technical, business, or financial information under this Task Order, it may be required to treat such information in accordance with any restrictions imposed on such information. The Contractor may use technical data it first produces under this Task Order for its private purposes consistent with the rights in data clause included in its GSA Schedule contract, the security clauses of this Task Order and any relevant clauses included in a resulting Task Order.

See FAR Part 9.5 for more information on Organizational Conflicts of Interest.

### **I.2.4 DISQUALIFICATIONS**

GSA has identified the following situations that will likely disqualify a Contractor from receiving an award under this or future Task Order due to an Organizational Conflict of Interest. The Contractor receiving a Task Order award will likely be considered to have a conflict of interest if it has:

- Substantially participated in the development of requirements or solicitations released by SSD and its contracting office.
- Other knowledge that would give the Contractor an unfair advantage in a related acquisition.

As a result of the Contractor's unique position in performing this Task Order, the Contractor will further agree that *due to the nature of this Task Order, the likelihood of being excluded from any solicitation issued by this office are high.* Business intelligence acquired from its unique position could give it an unfair advantage, or the appearance of an unfair advantage.

### **I.2.5 MITIGATION PLAN**

GSA will review any mitigation plan submitted to determine whether the plan fully and adequately addresses the potential organizational conflict of interest concern. As such, an offeror described above may be eligible for award with the appropriate mitigation plan. This should be done as soon as there is recognition of the possibility of an OCI, not only when an OCI triggering event actually occurs.

However, it would be advantageous for the Contractor to:

- Avoid assisting SSD with writing of requirements and or solicitations in which the Contractor may have an interest in participating.
- Avoid leakage of information from participants on this Task Order to proposal teams in the company, or to management, who might inadvertently transmit information to proposal teams in the company.

### I.3 FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) SOLICITATION CLAUSES

This task order incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address:

<https://www.acquisition.gov/far/>.

Clause No	Clause Title	Date
52.227-1	Authorization and Consent	(DEC 2007)
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement	(DEC 2007)
52.243-3	Changes-Time-and-Materials or Labor-Hours	(Sept 2000)
52.246-6	Inspection-Time-and-Material and Labor-Hour	(May 2001)
52.249-14	Excusable Delays	(Apr 1984)
52.251-1	Government Supply Sources	(APR 2012)

#### 52.204-2 Security Requirements (Aug 1996)

(a) This clause applies to the extent that this contract involves access to information classified “Confidential,” “Secret,” or “Top Secret.”

(b) The Contractor shall comply with—

(1) The Security Agreement ([DD Form 441](#)), including the *National Industrial Security Program Operating Manual* (DoD 5220.22-M); and

(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

(End of clause)

### **52.204-9 Personal Identity Verification of Contractor Personnel (Jan 2011)**

(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24 and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

(b) The Contractor shall account for all forms of Government-provided identification issued to the Contractor employees in connection with performance under this contract. The Contractor shall return such identification to the issuing agency at the earliest of any of the following, unless otherwise determined by the Government:

- (1) When no longer needed for contract performance.
- (2) Upon completion of the Contractor employee's employment.
- (3) Upon contract completion or termination.

(c) The Contracting Officer may delay final payment under a contract if the Contractor fails to comply with these requirements.

(d) The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts when the subcontractor's employees are required to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system. It shall be the responsibility of the prime Contractor to return such identification to the issuing agency in accordance with the terms set forth in paragraph (b) of this section, unless otherwise approved in writing by the Contracting Officer.

(End of clause)

### **52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.**

As prescribed in 4.2105(b), insert the following clause:

Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2019)

(a) Definitions. As used in this clause—

“Covered foreign country” means The People's Republic of China.

“Covered telecommunications equipment or services” means—

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

“Critical technology” means—

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

“Substantial or essential component” means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition. Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in Federal Acquisition Regulation 4.2104.

(c) Exceptions. This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement. (1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at <https://dibnet.dod.mil>. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at <https://dibnet.dod.mil>.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

### **52.217-9 Option to Extend the Term of the Contract (Mar 2000)**

- (a) The Government may extend the term of this contract by written notice to the Contractor within 10 days, provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.
- (b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
- (c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 5 years.

(End of clause)

## **I.4 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM) CLAUSES INCORPORATED BY REFERENCE**

The full text of a provision may be accessed electronically at GSAM website:

<https://www.acquisition.gov/gsam/gsam.html>.

Clause No	Clause Title	Date
552.203-71	Restriction on Advertising	(SEP 1999)
552.204-9	Personal Identity Verification Requirements	(OCT 2012)
552.216-74	Task-Order and Delivery-Order Ombudsman	(JAN 2017)
552.228-5	Government as Additional Insured	(JAN 2016)
552.232-1	Payments	(NOV 2009)
552.237-73	Restriction on Disclosure of Information	(JUN 2009)

### **552.204-70 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2019)**

Definitions. As used in this clause-

“Covered telecommunications equipment or services”, “Critical technology”, and “Substantial or essential component” have the meanings provided in FAR 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

Prohibition. Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Contractors are not prohibited from providing-

Solicitation#:47QTCB19P0006 QT3CDG Internal Security and System Security Assessment Support Services (ISSSAS)

A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

Representation. The Offeror or Contractor represents that it [ ] will or [ ] will not [Contractor to complete and submit to the Contracting Officer] provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract, order, or other contractual instrument resulting from this contract. This representation shall be provided as part of the proposal and resubmitted on an annual basis from the date of award.

Disclosures. If the Offeror or Contractor has responded affirmatively to the representation in paragraph (c) of this clause, the Offeror or Contractor shall provide the following additional information to the Contracting Officer--

All covered telecommunications equipment and services offered or provided (include brand; model number, such as original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

Explanation of the proposed use of covered telecommunications equipment and services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b) of this provision;

For services, the entity providing the covered telecommunications services (include entity name, unique entity identifier, and Commercial and Government Entity (CAGE) code, if known); and

For equipment, the entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known).

(End of clause)

### **552.217-71 Notice Regarding Option(s) (Nov 1992)**

The General Services Administration (GSA) has included an option to extend the term of this contract in order to demonstrate the value it places on quality performance by providing a mechanism for continuing a contractual relationship with a successful Offeror that performs at a level which meets or exceeds GSA's quality performance expectations as communicated to the Contractor, in writing, by the Contracting Officer or designated representative. When deciding whether to exercise the option, the Contracting Officer will consider the quality of the Contractor's past performance under this contract in accordance with 48 CFR 517.207.

(End of clause)

### **552.219-74 Section 8(a) Direct Award.**

As prescribed in 519.870-8, insert the following clause:

#### **Section 8(a) Direct Award (Sep 1999)**

(a) This contract is issued as a direct award between the contracting activity and the 8(a) Contractor pursuant to the Memorandum of Understanding between the Small Business Administration (SBA) and the General Services Administration. SBA retains the responsibility for 8(a) certifications, 8(a) eligibility determinations, and related issues, and will provide counseling and assistance to the 8(a) contractor under the 8(a) program. The cognizant SBA district office is:

[Complete at time of award]

Solicitation#:47QTCB19P0006 QT3CDG Internal Security and System Security Assessment Support Services (ISSSAS)

(b) The contracting activity is responsible for administering the contract and taking any action on behalf of the Government under the terms and conditions of the contract. However, the contracting activity shall give advance notice to SBA before it issues a final notice terminating performance, either in whole or in part, under the contract. The contracting activity shall also coordinate with SBA prior to processing any advance payments or novation agreements. The contracting activity may assign contract administration functions to a contract administration office.

(c) The Contractor agrees:

(1) To notify the Contracting Officer, simultaneous with its notification to SBA (as required by SBA's 8(a) regulations), when the owner or owners upon whom 8(a) eligibility is based plan to relinquish ownership or control of the concern. Consistent with 15 U.S.C. 637(a)(21), transfer of ownership or control shall result in termination of the contract for convenience, unless SBA waives the requirement for termination prior to the actual relinquishing of ownership and control.

(2) To the requirements of 52.219-14, Limitations on Subcontracting.

(End of clause)

**552.236-75 Use of Premises (Apr 1984)**

(a) If the premises are occupied, the Contractor, his subcontractors, and their employees shall comply with the regulations governing access to, operation of, and conduct while in or on the premises and shall perform the work required under this contract in such a manner as not to unreasonably interrupt or interfere with the conduct of Government business.

(b) Any request received by the Contractor from occupants of existing buildings to change the sequence of work shall be referred to the Contracting Officer for determination.

(c) If the premises are occupied, the Contractor, his subcontractors and their employees shall not have access to or be admitted into any building outside the scope of this contract except with official permission.

(End of clause)

**END OF SECTION I**

**SECTION J - LIST OF ATTACHMENTS**

**LIST OF ATTACHMENTS**

Attachment A	Security Solutions Branch Functional Responsibilities Matrix
Attachment B	ISSO Responsibilities Checklist
Attachment C	Request for Travel Authorization
Attachment D	Nondisclosure Agreements (NDAs) and Individual Conflict of Interest (COI)
Attachment E	Project Staffing Plan Template
Attachment F	Department of Defense Contract Security Classification Specifications (DD Form 254)

**END OF SECTION J**

## **SECTION K**

### **REPRESENTATIONS, CERTIFICATIONS, AND OTHER STATEMENTS OF OFFERORS**

#### **K.1 CONTRACT PROVISIONS**

##### **52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment.**

As prescribed in 4.2105(a), insert the following provision:

Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2019)

(a) Definitions. As used in this provision—

“Covered telecommunications equipment or services”, “Critical technology”, and “Substantial or essential component” have the meanings provided in clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Prohibition. Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Contractors are not prohibited from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Representation. The Offeror represents that—

It ☐ will, ☐ will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation.

(d) Disclosures. If the Offeror has responded affirmatively to the representation in paragraph (c) of this provision, the Offeror shall provide the following information as part of the offer

(1) All covered telecommunications equipment and services offered (include brand; model number, such as original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(2) Explanation of the proposed use of covered telecommunications equipment and services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b) of this provision;

(3) For services, the entity providing the covered telecommunications services (include entity name, unique entity identifier, and Commercial and Government Entity (CAGE) code, if known); and

(4) For equipment, the entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known).

(End of provision)

**Note: Incorporated in the STARS II GWAC**

**END OF SECTION K**

## **SECTION L - INSTRUCTIONS TO OFFERORS**

### **L.1 SUBMISSION OF QUESTIONS**

The contracting office shall be the sole point of contact for answering questions regarding the RFP. .

In posing questions, Contractors must cite the relevant section, paragraph, and page number. Questions should be written in a way that enables clear understanding of the Contractors' issues or concerns. Statements expressing opinions, sentiments, or conjectures are not considered valid inquiries and will not be receive a response. Further, Contractors are reminded that the Contracting Officer will not address hypothetical questions aimed at receiving a potential "evaluation decision."

### **L.2 GENERAL INSTRUCTIONS**

Offerors shall furnish the information required by this request for proposal (RFP). Proposals shall set forth full, accurate, and complete information as required by this solicitation package (including attachments).

Offerors submitting restrictive data within their proposals that they do not want disclosed to the public for any purpose or used by the Government except for evaluation purposes, shall mark the title page with the following legend:

"This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used or disclosed--in whole or in part--for any purpose other than to evaluate this proposal or quotation. If, however, a Task Order is awarded to this Offeror as a result of--or in connection with--the submission of this data, and the Government incorporates the proposal as part of the award, the Government shall have the right to duplicate, use, or disclose the data. Also, this restriction does not limit the Government's right to use the information contained in this data if it is obtained from another source without restriction. The data subject to the restriction is contained on pages (insert page numbers or other identification of documents)"; and

Mark each page that contains restrictive data with the following legend:

"Use or disclosure of data contained on this page is subject to the restriction identified on the title page of this proposal or quotation."

The Government assumes no liability for disclosure or use of unmarked data and may use or disclose the data for any purpose. Unless restricted, the information submitted in response to this request may become subject to disclosure to the public pursuant to the provisions of the Freedom of Information Act (5 USC. 551).

### **L.3.0 SUBMISSION INSTRUCTIONS**

#### **L.3.1 Government Property**

Upon receipt, all proposals become Government property and shall not be returned.

#### **L.3.2 Electronic Submission of Proposal**

The proposal shall contain the name, address, email and phone number of the POC authorized to represent the Contractor for this acquisition. Proposals shall be submitted in electronic format only; hard copies will not be accepted. Use separate electronic files for separating the technical response from the pricing response. If files are compressed, the necessary decompression program must be included. Please use unique and clear document file names. Proposals shall be submitted in a format readable by Microsoft (MS)

Word 2010 (Technical Proposal), MS Excel 2010 (Price Proposal), or Adobe PDF (any) as applicable.

Document/attachment size restrictions for the eBuy system is 5MB.

This RFP does not obligate the Government to pay any costs incurred in the submission of any offer or in making necessary studies for the preparation thereof, nor does it obligate the Government to procure or contract for said services.

#### **L.4.0 PROPOSAL FORMAT**

##### **L.4.1**

The proposal shall consist of the volumes listed below, which will be used during the evaluation process.

The proposal must address the requirements, provisions, terms and conditions, and clauses stated in all sections of the RFP. A proposal that restates the requirements or statements from this RFP, or just simply states that it is compliant with the RFP without providing a description of the approaches, techniques, or solutions may be considered unacceptable.

The Technical Volume shall be comprised of the Technical Approach and Program Management. The Price volume shall be in separate volume. The Technical Volume (Technical Approach and Program Management factors) is limited to 20 total pages (excluding resumes). . The Price Volume has no page limit, but shall be limited to pricing related information only.

##### **L.4.2**

Each volume shall be in English and marked with the solicitation number, title and offeror's name. Pages shall be numbered. The typewritten or printed letters shall be no smaller than 11 point Times New Roman/Arial, 1" margins around the printed page. The proposal submissions shall be in Microsoft Word, Excel, or electronic Adobe PDF format only.

##### **L.4.3 Technical Approach:**

At a minimum, the proposal must convey a thorough demonstration and understanding of cloud computing services, business requirements, functionality, and complexities and provide solutions to accomplish all aspects of the Program.

##### **L.4.4 Program Management:**

The Offeror's Program Management approach shall identify the various management approaches utilized to address the objectives in the RFP. Describe Quality Control Plan, SLAs, Customer Engagement, Key Personnel, Roles and Responsibilities, Staffing and Security, Personnel Resumes, relevant knowledge and experience, and availability of personnel in accordance with the instructions contained in the solicitation.

The vendor shall provide a description of the Quality Control Plan (QCP) that shall be used for this Task Order. The vendor shall be solely responsible for the supervision, management, and inspection of its employees under this PWS. The vendor shall monitor and ensure its employees meet all of the requirements of the solicitation. Demonstrate quality control and quality assurance methodology applicable to this engagement, and ensure the government has access to documented traceability and resource data in support of all processes articulated in the QCP.

The offeror shall provide a Project Staffing Plan (see Attachment "E") in whatever format the Offeror deems appropriate. The offeror will submit the proposed Project Staffing Plan which addresses the requirements contained in the RFP (Security, Key and non-key Personnel as applicable, Relevant Knowledge and Experience, Roles and Responsibilities, and availability of personnel will be indicated) to ensure that personnel are available, acceptable,

and suited to the work contained in the RFP. The submission shall contain all individuals who will be working on this effort.

The labor categories awarded under STARS II GWAC will be used to enable the Offeror to fulfill this requirement.

Resumes shall be submitted for all key personnel proposed, and shall clearly demonstrate that the offeror has the necessary personnel with the requisite knowledge, skills and experience to perform the required work in Section C of this RFP. Resumes will be reviewed for previous experience, aligning with Section H of this RFP. Indicate the length of time that key personnel have been involved in similar projects. Qualifications in the form of certifications, education and experience shall be submitted for all non-key positions (Roles and Responsibilities may be used in keeping with the 8(a) Stars II contract model).

A comprehensive Nondisclosure Agreement (NDA) will be required of each individual performing under this Task Order at the GSA location. The NDA will be signed before commencement of work under this Task Order.

#### **L.4.5 Price**

Labor hours used and hourly rates by labor category from the STARS II authorized pricing, less any offered discounts, shall be included in the Total Price. Descriptions of STARS II offered labor categories, including education and experience (or Roles and Responsibilities), shall be included in the Price Proposal. The labor categories awarded under STARS II GWAC will be used to enable the Offeror to fulfill this requirement.

DO NOT include technical documentation in the pricing volume. It will NOT be forwarded to the Technical Evaluation team. DO include information about offered labor categories including education and experience (or Roles and Responsibilities), and hourly rates, in the Pricing Volume.

**END OF SECTION L**

## **SECTION M - EVALUATION FACTORS FOR AWARD**

### **M.1.0 Evaluation Process**

The Government will make award, based on the proposal received, using the evaluation criteria provided below. The Government will consider the level of effort and the mix of labor proposed to perform the specific tasks being ordered, and will determine the reasonableness of the proposed price. Non-price factors will be evaluated for adherence to the requirements found in Section C of the solicitation.

The three (3) Evaluation factors are comprised of:

**Factor 1** – Technical Approach;

**Factor 2** – Program Management; and

**Factor 3** – Price. Price is a stand alone factor.

#### **M.1.1 Factor 1: Technical Approach**

The Technical Approach shall demonstrate the offeror understands the Government's requirements and the offeror's capability to perform the prospective task order. At a minimum, the technical proposal must reflect a thorough demonstration and technical understanding of the PWS requirements as cited in Section C of the RFP.

#### **M.1.2 Factor 2: Program Management**

The technical proposal shall also include details on the Program Management approach per the PWS requirements cited in Section C of the RFP. The Government will review the program management approach to ensure the offeror has a thorough understanding of the requirements.

All components of the Program Management proposal, including Quality Control Plan, Key Personnel, Roles and Responsibilities, Staffing and Security, Personnel Resumes, relevant knowledge and experience, and availability of personnel will be evaluated to ensure that they are complete, acceptable and responsive to the instructions contained in the RFP.

The offeror shall identify proposed "Key Personnel". Resumes must reflect that the proposed personnel meet the proposed management plan in the area of associated responsibilities and partnerships between Government organizations and the offeror.

#### **M.1.3 Factor 4: Price**

The Offeror's price proposal will be evaluated to ensure that it complies with all requirements provided in this RFP. The evaluation will determine the reasonableness of the individual rates and total price proposed.. The total price shall include the base year and all option years, a total of four (4) years.

Labor categories proposed in response to this RFP shall be proposed from the offeror's STARS II GWAC in accordance with the instructions in this section. The offeror is encouraged to offer additional discounts to their GWAC hourly rates in response to this solicitation.

The offeror shall complete all of the pricing tables in Section B, at a minimum, for the requirements which will be used to determine the total evaluated price. The offeror is responsible for providing information on the rationale of the proposed price.

Solicitation#:47QTCB19P0006 QT3CDG Internal Security and System Security Assessment Support Services (ISSAS)

NOTE: The proposal must address the requirements, provisions, terms and conditions, and clauses stated in all sections of the RFP. A proposal that restates the requirements or statements from this RFP, or just simply states that it is compliant with the RFP without providing a sufficiently detailed description of the approaches, techniques, or solutions may be considered unacceptable.

**M.2 BASIS FOR AWARD**

**END OF SECTION M**

**END OF THE SOLICITATION**